Attachment J.17

WAN EMERGENCY NOTIFICATION PROCEDURES
Revised July 2000

INTRODUCTION

The Information Resources Management Office (IRMO) and the Information Systems Security Officer (ISSO) recommends the following emergency notification procedures to inform users, and managers of potential threats or disruptions to network operations.

Situations that require notification include both threatening and non-threatening emergencies. Any emergency situation that could extend to multiple sites would be a threatening emergency. A localized disruption in service that does not have the potential of spreading to other sites would be a non-threatening emergency.

Threatening emergencies include:

Malicious code present on a file server or on 2 or more workstations

Malicious code detected anywhere, if in "stealth virus" category

Simultaneous power outage during normal working hours in more than one location

Threats of violence, such as a bomb threat

Power failure not resolved by backup power supply

Non-threatening emergencies include:

Power outages other than at the Clifton campus disrupting service for more than 2 hours

Disruptions in e-mail and scheduling systems for more than 2 hours during normal working hours

PROCEDURES FOR THREATENING EMERGENCIES

See Appendix A for Detailed Threatening Emergencies Notification Procedures

ATSDR and each CDC CIO should designate a primary and a secondary contact

for notifications. Each local area network should also designate a primary and secondary contact. Either the primary or secondary contact at each level should be reachable at all times by telephone or by alphanumeric pager. IRMO and the ISSO will maintain a list of contacts with telephone and pager numbers. ATSDR and CDC CIO contacts should maintain a list of their LAN contacts with telephone numbers and pager numbers. Users should also be aware of, and have access to, the names, telephone numbers, and pager numbers of a primary and secondary contact for the LAN and their organization. The contact in CHM and the ISSO should be contacted as soon as possible with a verbal notification. A similar notification procedure should be implemented at the CIO level. Each LAN should have a primary and secondary contact person. The organizational contact should notify each LAN contact verbally and send a group alphanumeric pager message.

PROCEDURES FOR NON-THREATENING EMERGENCIES

The procedures are similar for non-threatening emergencies.

Notification Messages

The content of notification messages would vary according to the type of emergency. For all emergencies the message should contain the following information, if known:

Geographic, organizational, and network location(s)

Beginning time of emergency

For disruption of services, expected time of resolution

Extent of the emergency or disruption (Detailed information is essential, as others are trying to judge what additional response(s) may be needed.)

For virus infections, this message should also contain:

Name and description of the virus

Name of the software that was used to detect the virus

Name of the software that was used to clean the virus

Route of introduction, if available

Information for Users

1. Users should be aware of the names, telephone numbers, and pager numbers of a primary contact and secondary contact for the LAN and for the organization to which they belong.

2. Server based Malicious code monitoring software, such as, McAfee AntiVirus and Norton AntiVirus should be configured to broadcast a warning message to a select group of users. This group should verify that appropriate contacts are aware of the problem.

3. Workstation virus monitoring software, such as, McAfee AntiVirus and Norton AntiVirus should display a warning message that includes the names, telephone numbers, and pager numbers of the contacts.

On-line information

Information on viruses, security loopholes, and other potential threats should be maintained in the CDC WAN Emergency Announcements public folders. CDC should subscribe to a database of current viruses. Information from users and technical staff should be sent by E-mail to the ISSO and to the IRMO notification mailbox for verification and possible posting in the system.

CDC WAN Emergency Announcement Public Folder Procedures

The person detecting the virus or potential threat should notify their respective IRM Coordinator (http://intranet.cdc.gov/irmo/irmointra/irmcoord.htm), and the CDC ISSO/IRMO/Virus Notification Group providing all the information they have regarding:

Name of person detecting virus or potential threat and date detected

Name and description of virus or potential threat

Name of the software that was used to detect the virus

Name of the software that was used to clean the virus

Route of introduction, if available

Members of the CDC ISSO/IRMO Virus Notification group have posting rights to the CDC WAN Emergency Announcements public folders. This group is responsible for verifying that the virus or potential threat is not a hoax before posting the above information in the public folder. If valid, the information or threat should be posted in the public folder by the ISSO

within 24 hours. If not posted within 24 hours, NTB will assume that the ISSO is not available and be responsible for posting. Postings to the CDC WAN Emergency Announcements public folder will automatically generate an e-mail to the CHM Emergency Notification POC's distribution list which will be maintained by CHM.

Information posted to the CDC WAN Emergency Announcements public folders will automatically expire after 90 days.

Tracking Information

Information on security incidents, malicious code incidents (threatening and non-threatening), and any other WAN related emergencies should be maintained in a tracking system that can be used to evaluate the security status of our network and computer resources.

enotify.wpd

3/22/96

Updated 10/18/99

Updated July 2000

APPENDIX A

Computer & Hi-tech Management, Inc. (CHM) Contractor Support

Threatening Emergencies Notification Procedures

Purpose

This document establishes the emergency reporting and notification procedures to inform users and administrators of equipment failures, virus infections, breaches of information security, and potential threats or disruptions to CDC network operations. Any CDC IRM Manager, user, or designated point of contact may make the initial call. If an organization desires only certain individuals to contact CHM, this should be set forth in a local policy.

Notification Procedures and Actions

Normal Workhours (Monday through Friday 7:30 AM - 5:00 PM)

1. Any CDC IRM Manager, user, or other designated point of contact may call

the CHM Help Desk at 678-547-0311 and provide the information indicated below:

a. Name and telephone number of person calling.

b. Geographic, organizational, and network location(s) affected.

c. Nature of the emergency (If the emergency involves a virus or other malicious code infection, the caller should provide the time the virus was detected, the name and description of the virus, the scope of the infection, and the name of the software used to detect and/or clean the virus).

2. CHM will accomplish the following actions:

a. Open a Service Call for problem tracking and to record problem resolution.

b. Dispatch support personnel to resolve the reported problem.

c. If the problem involves a virus/malicious code infection or a breach of information security, notify the Information Systems Security Officer (ISSO), the Information Resources Management Office (IRMO) and appropriate Centers, Institutes and Offices (CIOs) via telephone and E-Mail. A list of Points of Contact will be provided separately.

Nights, Weekends, and Holidays

1. Any CDC IRM manager, user, or other designated point of contact who requires contractor assistance or has an emergency situation to report should call CHM at pager number 678-751-9884. The customer should provide:

a. Name and telephone number of the person calling.

b. Building location and organization.

c. Nature of the problem or emergency (If the emergency involves a virus/malicious code infection, the caller should provide the time the virus was detected, the name and description of the virus, the scope of the infection, and the name of the software used to detect and/or clean the virus).

2. During non-duty hours when a server fails the affected LAN Administrator and a CHM Manager will receive simultaneous notification via WINBEEP. The CHM Manager will wait ten minutes to receive a call from the LAN

Administrator to confirm that he or she has received the WINBEEP notification. If no confirming call is received within ten minutes, the CHM Manager will attempt to contact the LAN Administrator and/or other designated point of contact for that CIO via telephone using the CHM Emergency Notification Points of Contact list provided by CDC.

3. In either of the above cases, CHM will accomplish the following actions:

a. In cases of equipment failures, notify the designated organizational point of contact via WINBEEP and E-Mail. When the organizational point of contact responds, the CHM manager will ascertain if contractor support is required, and if so, will contact an appropriate contractor employee and determine a time when that person will arrive at the work site. The CHM Manager will then call the organizational point of contact and provide the name and expected arrival time of the contractor employee.

b. In cases of virus or malicious code infection or breach of information security, notify the ISSO, IRMO, and other organizations as required via WINBEEP and E-Mail.

4. When a CDC virus notification is broadcast to voice mail group code 024, the message will be deposited in a "phantom" email mailbox created for CHM (329-1066). This email mailbox is set up to automatically contact CHM's emergency pager (678-751-9884) and then display the mailbox # (1066). John Spencer (CHM) is going to notify his managers that anytime a pager displays "1066" they should call 404 302-2000 and access mailbox 329-1066 which will contain the message.